IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

Application No.:	**09/872,077**	Confirmation No.	**3841**
Applicant:	**Amini et al.**	Filed:	**November 16, 2004**
Art Unit:	**2134**	Examiner:	**Andrew L. Nalven**
Docket No.:	**STL920000116US1**	Customer No.:	**55070**
Title:	**Systems, Methods, and Computer Program Products for Accelerated Dynamic Protection of Data**		

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

SUMMARY OF INTERVIEW HELD ON FEBRUARY 23, 2007

S I R:

Applicants thank Examiner Nalven for the Examiners Interview on February 23, 2007.

This communication provides Applicants Summary of the Interview held on February 23, 2007.

March 23, 2007

Janet M. Skafar
Reg. No. 41,315
Attorney for Applicants
(650)988-0655

Participants in the Interview with Examiner Nalven:

Janet M. Skafar, Esq.; and William Belknap, Inventor

Claims discussed: Claims 7 and 10

General Thrust of the Principal Arguments

Applicants generally argued that the Shimomura patent does not teach the encryption state of claim 7.

Applicants generally argued that with respect to claim 10, that modifying the Mitty patent to use an untrusted intermediary would render the Mitty patent unsatisfactory for its intended purpose.

APPLICANTS INTERVIEW SUMMARY

**PROPOSED AMENDMENTS TO CLAIMS
FOR DISCUSSION PURPOSES ONLY AT INTERVIEW
NOT FOR ENTERING**

7. (currently amended) A computer implemented method for encrypting ~~a data element~~ and decrypting ~~said data element~~ using a first ~~static~~ key and a second ~~dynamic~~ key, comprising:

encrypting a ~~said~~ data element with said first ~~static~~ key and an encryption state to produce a first encrypted data, wherein said encrypting maintains said~~an~~ encryption state;

encrypting said first encrypted data ~~element~~ with said second ~~dynamic~~ key to produce a second encrypted data;

transmitting said second encrypted data ~~element~~ with said encryption state to a receiving computer system;

~~decrypting said encrypted data element with said static key and said dynamic key on said receiving computer system;~~

determining, by said receiving computer system, whether transmission of a previous second encrypted data ~~element~~ failed; and

in response to said determining ~~said transmission of said previous encrypted data element failed~~, said receiving computer system:

decrypting said second encrypted data ~~element~~ with said second key, and

decrypting said decrypted second encrypted data with said first ~~static~~ key and[[,]] said encryption state transmitted with said second encrypted data ~~element~~ to produce a decrypted data element, ~~and said dynamic key~~ without retransmission of said previous second encrypted data ~~element~~, without recovering said previous second encrypted data.

APPLICANTS INTERVIEW SUMMARY

PROPOSED AMENDMENTS TO CLAIMS FOR DISCUSSION PURPOSES ONLY AT INTERVIEW NOT FOR ENTERING

10. (currently amended) The method of Claim 7, f~~urther comprising:~~

wherein said encrypting said data element with said first ~~static~~ key is on a first computer system;

further comprising: transmitting said first encrypted data ~~element~~ from said first computer system to a second computer system;

wherein said encrypting said first encrypted data ~~element~~ with said second ~~dynamic~~ key is on said second computer system, said second computer system being untrusted; and

thereby distributing encryption and decryption between said first computer system, said second computer system, and said receiving computer system.